Management System: Information Resource Management

Subject Area Description: Cyber Security (and Personally Identifiable Information [PII])

Policy: Control of Unclassified Electronic Information

Management System Owner: Ward Best
Subject Matter Expert: Lisa Rawls

Issue Date: 12/16/2015
Revision: 0

1.0 Purpose

The purpose of this policy is to define the use and control of all Unclassified Electronic Information at the Environmental Management Consolidated Business Center (EMCBC) and the reporting requirements for loss of control of Controlled Unclassified Information (CUI).

2.0 Scope & Applicability

This policy is applicable to all electronic media managed by the EMCBC directly or by Service Level Agreement. This policy is not applicable to Classified Electronic Information.

3.0 General Information

3.1 Policy**:** It is the policy of the EMCBC that all electronic information is controlled as required. All forms of electronic information will be reviewed for sensitivity and applicable controls will be applied. Applicable controls come from the references listed in Section 4.0 of this policy. Excessive controls are cumbersome and unduly impact business operations and are to be avoided. Where data types are mixed, the most stringent control shall apply.

3.2 Data Sensitivity and Controls**:** Data within the EMCBC network is classified by type according to the sensitivity of the data.

3.2.1 Type I Data: The data in this category requires the most stringent control and is made up of the most sensitive data. All CUI falls into this category. Other

data may be designated as Type I by the Content Owner if necessary to meet a particular need. These controls mandate:

- All CUI shall be stored on network peripherals, not on Desktops.
- All data stored on laptops, USB drives, CDs, and DVDs shall be encrypted.
- All CUI stored on mobile devices including portable hard drives shall be encrypted.
- All laptops will use full-device encryption.
- CUI is encrypted before transfer over open connections. EMCBC uses Entrust for this purpose.
- Data access within the accreditation boundary is controlled through network authentication.
- Remote access to EMCBC file storage and applications containing CUI shall utilize two-factor authentication and conform with the time-out requirements of the references listed in Section 4.0.

3.2.1.1 Personally Identifiable Information (PII) is a special form of Type I data and requires additional controls over and above those already stated.

- PII is not permitted to be stored on Desktop computers, laptops, USB drives, DVDs, CDs or any other form of portable media. In unusual circumstances PII may be stored on portable media with the written authorization of the EMCBC Director or designee. Such authorizations will expire after 90 days, at which time the media will need to be returned to IRM for disposition, or renewal of the authorization is required. Personnel authorized to transport such data will be required to receive additional training to ensure a full understanding of the ramifications of transporting PII.
- Annual Cyber Security Awareness training, required for all users, will describe PII in detail to provide a clear understanding of the special restrictions and rigorous reporting requirements for PII.

3.2.2 Type II Data: Information in this category is designated by the Content Manager or Content Owner. The data is usually made up of sensitive business information that, if compromised, could lead to an unfair competitive advantage, divulge sensitive legal position, or expose other confidential information. The Content Owner is responsible for the designation of all Type II data. The following controls apply:

- Data access within the accreditation boundary is controlled through network authentication.

- All data stored on laptops shall be encrypted.
- USB Drives and other portable media shall be protected by encryption.
- Remote access to EMCBC file storage and applications containing Type II data shall utilize two-factor authentication and conform to the time-out requirements of the references listed in Section 4.0.

3.2.3 Type III Data: Information in this category is designated by the Content Manager or Content Owner. The goal of this is to protect data integrity and add a level of confidentiality, or screen information from the general public. Certain types of Business Sensitive Data may fall into this category. The following controls apply:

- Data access within the accreditation boundary is controlled through network authentication.
- USB Drives and other portable media shall be protected by encrypting the device with Lumension Endpoint Security.
- Remote access shall require two-factor authentication.

3.2.4 Type IV Data: Information that is or can be made available to the general public without restriction. Data integrity to ensure accurate communications is the goal of this information control. The following controls apply:

- Data access within the accreditation boundary is controlled through network authentication.
- Data posted to websites are controlled by the Content Owner or Content Manager.
- Data integrity for web servers and other public facing information systems is maintained by the security controls imposed by the System Owner as part of the Accreditation Boundary.

3.3 Reporting of Data Security Issues**:** All users responsible for the control or transportation of Type I and Type II Data shall immediately report any loss or potential compromise of the data to the ADIRM. (Note: This reporting shall be done within 30 minutes of any possible loss or breach of PII Data.) All responses to loss of data control will be handled by IRM in accordance with Incident Response procedures.

3.4 Training**:** All users handling Type I and Type II Data shall receive specific training in the use of encryption and data protection systems. All laptop users will receive training on the use of laptop locking and encryption devices and systems. General User training will address the controls for Type III and Type IV Data.

Summary Chart on Controls for Electronic Information

Type	Definition	Control
I-PII	Data defined as PII by regulation or requirement.	Data is only stored on network storage devices. Access is controlled by network credentials. Special authorization required for transportation on mobile devices. Users receive special training to ensure protection of this data.
I	Data that has been specifically defined as needing encryption by requirement such as Sensitive Unclassified Information.	Data is stored or transported encrypted as required and requires two-factor authentication for remote access. Users receive special training to ensure protection of this data.
II	Business Sensitive Data – Data that has a direct bearing on business decisions that if compromised could result in an unfair advantage to parties conducting business or in legal action with the Department. Type II data is designated by the Content Owner.	Data access is controlled through the network and requires two-factor authentications for remote access. Data is protected by encryption in transport.
III	Information about Business Sensitive Data that requires protection to ensure data integrity and a level of confidentiality, or data that needs to be screened from the general public. Type III data is designated by the Content Owner.	Data access is controlled through the network and requires two-factor authentication for remote access. Files transported on removable media should be protected by password.
IV	Public data that may be released at any time. Web site data makes up the bulk of this data.	Data access is controlled through the network. Data is posted to the web as directed by the Content Manager. Precautions are taken to ensure data integrity.

4.0 References

4.1. Office of Management and Budget Memorandum M-06-16, Protection of Sensitive Agency Information, dated June 23, 2006

4.2. DOE O 205.1B, Department of Energy Cyber Security Program

4.3. DOE EM Risk Management Approach Implementation Plan (RMAIP)

4.4. EMCBC IMP-IRM-8308-03, Software Application Development and Management

4.5. EMCBC PP-IRM-240-08, Cyber Security – System Security Plan (SSP) for General Support System (GSS)

4.5.1 AC-19, Access Control for Mobile Devices
4.5.2 MP-4, Media Storage
4.5.3 MP-5, Media Transport

5.0 Definitions – Definitions are located at the top of the Management System Description page.

EMCBC RECORD OF REVISION

Document Title: DIGITAL AUTHORIZATION IN APPLICATIONS AND DATABASES

If there are changes to the controlled document before the two-year review cycle, the revision number stays the same; one of the following will indicate the change:

l Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised, or

l Placing the words GENERAL REVISION at the beginning of the text. This statement is used when entire sections of the document are revised.

If changes and updates occur at the two-year review cycle, the revision number increases by one.

Rev. No.	Description of Changes	Revision on Pages	Date
0	Format revision	N/A	12/16/15